REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-20 are presently pending in this case. Claims 1, 3, 6, and 8 are amended and new Claims 13-20 are added by the present amendment. As amended Claims 1, 3, 6, and 8 and new Claims 13-20 are supported by the original disclosure,[1] no new matter is added.

In the outstanding Official Action, Claim 1 was rejected under 35 U.S.C. §101; Claim 1 was rejected under 35 U.S.C. §112, second paragraph; Claims 1, 2, 5, 6, 9, and 11 were rejected under 35 U.S.C. §102(b) as anticipated by Garib (U.S. Patent No. 6,728,378); Claims 3 and 4 were rejected under 35 U.S.C. §103(a) as unpatentable over Garib in view of Kaufman et al. (U.S. Patent No. 5,764,772, hereinafter "Kaufman"); Claim 7 was rejected under 35 U.S.C. §103(a) as unpatentable over Garib in view of Kitamura (U.S. Patent Application Publication No. 20020016917); Claim 8 was rejected under 35 U.S.C. §103(a) as unpatentable over Garib in view of Kitamura and further in view of Kaufman; Claim 10 was rejected under 35 U.S.C. §103(a) as unpatentable over Garib in view of Schneier (Applied Cryptography, Second Edition); and Claim 12 was rejected under 35 U.S.C. §103(a) as unpatentable over Garib in view of Inada (U.S. Patent No. 6,986,044).

With regard to the rejection of Claim 1 under 35 U.S.C. §101, Claim 1 is amended to recite "public key encryption processing means for performing an encryption operation on data using a public key encryption technique to generate encrypted data." The generation of encrypted data by the public key encryption processing means is respectfully submitted to be a useful, concrete, and tangible result. Accordingly, it is respectfully submitted that Claims 1-12 are in compliance with all requirements under 35 U.S.C. §101.

[1]See, e.g., the specification at page 37, lines 2-21.

With regard to the rejection of Claim 1 under 35 U.S.C. §112, second paragraph, Claim 1 is amended to recite "control means for controlling the hash value generation means and the public key encryption processing means, the control means suppressing arithmetic operations performed by the public key encryption processing means when the hash value generation means accesses the storage means." Thus, the phrase "other arithmetic operations" is no longer used. Accordingly, it is respectfully submitted that Claims 1-12 are in compliance with all requirements under 35 U.S.C. §112, second paragraph.

With regard to the rejection of Claim 1 as anticipated by Garib, that rejection is respectfully traversed.

Amended Claim 1 recites in part, "control means for controlling the hash value generation means and the public key encryption processing means, the control means suppressing arithmetic operations performed by the public key encryption processing means when the hash value generation means accesses the storage means."

Garib describes a secret key messaging apparatus that securely transmits and receives electronic mail. Garib describes that a hashing algorithm may be used to determine if a received message has been tampered with.[2] Further, information may be encrypted with secret-key or symmetric-key encryption.[3] In this regard, Garib describes a statement issuing computer system 101 that includes a password providing means 107 that applies a password hashing algorithm to a password.[4] Statement issuing computer system 101 of Garib also includes message preparation means 112 that encrypts an electronic mail message.[5] However, there is no teaching or suggestion in Garib for any device that suppresses arithmetic operations performed by the message preparation means 112 when the password providing means 107 accesses data storage. The portion of Garib cited for this feature in the

[2]See Garib, column 3, lines 46-52.
[3]See Garib, column 4, lines 27-42.
[4]See Garib, column 11, lines 37-40.
[5]See Garib, column 12, lines 16-21.

outstanding Office Action, column 4, lines 9-26, only describes that hash vales can be used to protect passwords. This portion of Garib does not mention encryption at all, and certainly does not mention "control means" as defined in amended Claim 1. Thus, it is respectfully submitted that Garib does not teach "control means" as defined in amended Claim 1. Consequently, Claim 1 (and Claims 2-12 dependent therefrom) is not anticipated by Garib and is patentable thereover.

With regard to the rejection of Claims 3 and 4 as unpatentable over Garib in view of Kaufman, it is noted that Claims 3 and 4 are dependent from Claim 1, and thus are believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Kaufman does not cure any of the above-noted deficiencies of Garib. Accordingly, it is respectfully submitted that Claims 3 and 4 are patentable over Garib in view of Kaufman.

With regard to the rejection of Claim 7 as unpatentable over Garib in view of Kitamura, it is noted that Claim 7 is dependent from Claim 1, and thus is believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Kitamura does not cure any of the above-noted deficiencies of Garib. Accordingly, it is respectfully submitted that Claim 7 is patentable over Garib in view of Kitamura.

With regard to the rejection of Claim 8 as unpatentable over Garib in view of Kitamura and further in view of Kaufman, it is noted that Claim 8 is dependent from Claim 1, and thus is believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Kitamura and Kaufman do not cure any of the above-noted deficiencies of Garib. Accordingly, it is respectfully submitted that Claim 8 is patentable over Garib in view of Kitamura and further in view of Kaufman.

With regard to the rejection of Claim 10 as unpatentable over Garib in view of Schneier, it is noted that Claim 10 is dependent from Claim 1, and thus is believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that

Schneier does not cure any of the above-noted deficiencies of Garib. Accordingly, it is respectfully submitted that Claim 10 is patentable over Garib in view of Schneier.

With regard to the rejection of Claim 12 as unpatentable over Garib in view of Inada, it is noted that Claim 12 is dependent from Claim 1, and thus is believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Inada does not cure any of the above-noted deficiencies of Garib. Accordingly, it is respectfully submitted that Claim 12 is patentable over Garib in view of Inada.

New Claims 13-20 are supported at least by original Claims 1-8. New Claim 13 recites in part, "a control unit configured to control the hash value generation unit and the public key encryption processing unit, the control unit configured to suppress arithmetic operations performed by the public key encryption processing unit when the hash value generation unit accesses the storage unit."

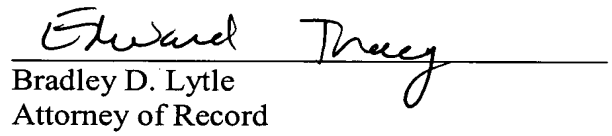
As noted above, there is no teaching or suggestion in Garib for any device that suppresses arithmetic operations performed by the message preparation means 112 when the password providing means 107 accesses data storage. Thus, it is respectfully submitted that Garib does not teach "a control unit" as defined in new Claim 13. Consequently, new Claim 13 (and Claims 14-20 dependent therefrom) is not anticipated by Garib and is patentable thereover.

Accordingly, the pending claims are believed to be in condition for formal allowance.

An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Edward W. Tracy, Jr.
Registration No. 47,998

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\ET\241199US\241199US-AMD5.21.07.DOC